HOLYROOD {CONNECT}

Public
Sector
Cyber Security

SCOTLAND

Published on *Cyber Security 2020* (https://cybersecurity.holyrood.com)

Agenda

Cyber Security Agenda

08:45	**Registration, Exhibition and Networking**
09:30	**Welcome and Introduction from the Chair** **Chelsea Jarvie**, Cyber Security Consultant
Session 1	**Current Policy and Latest Threat Analysis**
09:35	**Cyber Threats Know No Borders: Learning From Estonia** Estonia has become one of the leading nations in cyber security. Both the NATO Cooperative Cyber Defence Center of Excellence and the EU IT Agency are situated here in Tallinn. The main purpose of the cyber defence policy is to help ensure people's trust in the information society and avoid the loss of data. How Estonia is leading the way? **Anett Numa**, Expert Speaker, e-Estonia Briefing Centre
09:55	**Why Understanding Your Attack Surface Matters** What does it mean to obtain and use 'cyber intelligence' in a manner that effectively prioritises scarce resource across the full spectrum of 'Assess, Protect, Detect & Respond' cybersecurity disciplines? Threats in cyber-space arise for two main reasons; weakness in IT infrastructure and an interest taken by an attacker. Most businesses know they must mitigate cyber-threats for their own good but also because regulators require them to. Ensuring an organisation has the skills, agility and underlying platforms and processes to understand, detect and manage cyber-threats is one of the most compelling challenges faced by any business. Regulatory changes have pushed this issue up to board level. What should the priority be for an organisation that wants to improve its cyber security posture, finding and removing vulnerabilities in its infrastructure or assessing the external threats it faces? **Wicus Ross**, Senior Research Lead, SecureData

10:15	**Main Stage Panel Discussion** Delegates will hear from a panel of experts from Scotland, the wider UK and further afield on the latest threats, and how these developments might affect Scotland's public sector. **Wicus Ross**, Senior Research Lead, SecureData **Anett Numa**, Expert Speaker, e-Estonia Briefing Centre **Keith Nicholson**, Chair, Cyber Security Scotland
11:00	**Exhibition, Networking and Refreshments**
Session 2	**Breakout Sessions** During this session, delegates will pre-register for two of four workshops led by industry experts and focused on steps for embedding cyber-resillience within your organisation.
	Breakout A with OneTrust: Overcoming Today's Most Pressing Third-Party Risk Management Challenges • Review the drivers and challenges organizations face when managing third-party vendor risk • Identify priorities before, during and after vendor procurement • Takeaway a six-step approach for automating the third-party vendor risk lifecycle • Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk **Chris Paterson,** Solutions Engineer, OneTrust
	Breakout B with Sophos: Hacking is the New Malware: Why Everyone Is Now A Target The past 5 years have shown a dramatic shift in the tactics of cybercriminals. With the advent of ransomware and the ability to monetize any breach, criminals are aggressively targeting and hacking anyone and everyone. Sophos' Greg Iddon gives an overview of today's threat landscape and demonstrates how easy today's attackers have it. **Greg Iddon**, Senior Manager, Product Team, Sophos
	Breakout C: NHS Scotland - Embracing The Cloud and Meeting Its Security Demands Cloud computing is transforming the healthcare industry - helping staff to access data in real time, giving the public the capacity to obtain their own data more easily, and opening up new possibilities for research on the sector. But one of the biggest setbacks to cloud adoption is the possible security risk associated with storage and accessing sensitive data. **Deryck Mitchelson**, Director of National Digital and Information Security, NHS National Services for Scotland *Sponsored by Check Point*
	Breakout D with Check Point: Securing The Future, Protecting The Past This breakout session will cover approaches to securing sensitive data environments within the Public Sector. The focus will be on recent security developments in areas such as cloud, protecting mobile devices and IOT environments and will discuss best practices for enhancing an organisations Cyber Security posture. **Mark Mitchell**, Security Engineer, Check Point Software Technology

	Breakout E with Egress: Predicting The Unpredictable: How You Can Prevent Email Data Breaches People leak data every day. They are prone to making mistakes and behaving unpredictably, and as almost every employee has access to email, it's one of the most at-risk applications for modern enterprise organisations. As the rise in email data breaches shows, static email security solutions can't keep pace with this growing threat and are failing to protect sensitive information. So, how is it possible for CISOs and security professionals to predict the unpredictable, and mitigate this risk? Join this presentation to understand the psychology behind insider data breaches; how traditional technologies have failed to mitigate this threat; and the role of emerging technology, such as contextual machine learning, to empower employees to work more securely and prevent email data breaches. **George Kitchen**, Government Account Executive, Egress
11:25	**First Breakout**
12:05	**Transition**
12:15	**Second Breakout**
12:55	**End of Breakouts**
13:00	**Ministerial Address** **Kate Forbes MSP**, Minister for Public Finance and Digital Economy, Scottish Government
13:15	**Lunch, Exhibition and Networking**
13:30	**Demo Zone: Mindhunter: SonicWall's Two-Week Conversation with a Modern Ransomware Cell** Generally, people believe the size of their organization is what matters to hackers. In reality it is a vulnerability that attracts them, and it is an organization's security posture that will make hackers attack or retreat. Join SonicWall security expert Colin Gracie as he gives you an inside look into the human-side of a modern ransomware cell, their advice on how to stop them from infiltrating your organization, encrypting your endpoints, and spreading to other drives and segments of your network. **Colin Gracie**, Enterprise Security Specialist, SonicWall
Session 3	**Themed Panels - Preventing and Responding to Cyber Attacks** Building on the earlier Breakout Sessions, delegates will hear from a range of experienced panelliests drawn from across the public sector as they exchange best practice and discuss innovative solutions to common cyber challenges. Attendees will have the choice of two exciting panels for which they can pre-register.
14:05	**Panel A: Staff Behaviour Change and Embedding Good Cyber Hygiene** **Chair: Chelsea Jarvie**, Cyber Security Consultant **Jordan Schroeder**, CISO, HEFESTIS **Garry Scobie**, Deputy CISO, University of Edinburgh **Deryck Mitchelson**, Director of National Digital and Information Security, NHS National Services for Scotland **Chris Pinder**, Chief Operating Officer, IASME Consortium

14:05	**Panel B: Incident Response and Management** **Chair: Keith McDevitt**, Cyber Resilience Integrator, Scottish Government **Carol Peters**, Cyber Security Architect, Renfrewshire Council **Eamonn Keane**, Head of Cyber Security & Innovation, Scottish Business Resilience Centre **Emily Beeney**, Cyber Analytics Lead, Morgan Stanley **Charles Fraser**, Executive Principal Consultant, NCC Group
14:55	**Exhibition, Networking and Refreshments**
Session 4	**Horizon Scanning: Future-Proofing Scotland's Cyber Security** In the final session of the day, delegates will hear from three high-profile speakers on the steps Scotland's public sector can take to future-proof against future cyber-attacks. Topics including developing the workforce, building partnerships between the public, private and third sectors, and the intersection between cyber-security and emerging technologies such as Internet of Things.
15:15	**Developing a Cyber Cluster for Scotland** • Cyber Cluster- what do we mean by this? • Benefits of growing the community - what does this mean for you? • Leveraging the opportunities for collaboration across the ecosystem **Ciara Mitchell**, Head of Cyber, ScotlandIS
15:35	**Full Spectrum Cloud Native Security** Increasingly when businesses move their applications to the cloud they are going cloud native. There are however, some intersting security challenges around developing, deploying, testing, operating and investigating crimes in cloud native applications. This presentation aims to give a brief introduction to the full spectrum of cloud native security challenges. **Mark Hutchings**, Cyber Security Technical Consultant, QA Ltd
15:55	**Cyber Resilience and the Internet of Things** Internet of Things (IoT) technologies are enabling transformational benefits for organisations. However, cyber security threats associated with IoT are evolving rapidly with the increasing levels of IoT adoption. This presentation will provide an overview of IoT, addressing cyber security for solutions based on these technologies and how to ensure organisations build IoT cyber resilience. **Cade Wells**, Cyber Security Lead and Business Development Manager, CENSIS
16:15	**Questions and Comments**
16:40	**Chair's Closing Remarks** **Chelsea Jarvie**, Cyber Security Consultant
16:45	**Close of Conference**